(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 October 2003 (30.10.2003)

PCT

(10) International Publication Number
WO 03/090046 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/GB03/01466

(22) International Filing Date: 2 April 2003 (02.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0208916.7 18 April 2002 (18.04.2002) GB

(71) Applicant *(for all designated States except US)*: **ISIS INNOVATION LIMITED** [GB/GB]; Ewert House, Ewert Place, Summertown, Oxford OX2 7SG (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HEASMAN, John** [GB/GB]; 4, Surrey View, Roundabout Road, Copthorne, Crawley RH10 3LD (GB). **MOYLE, Steve** [GB/GB]; 1, Summerfield Road, New Hinksey OX1 4RU (GB).

(74) Agent: **STRACHAN, Victoria, Jane**; Urquhart-Dykes & Lord, Alexandra House, 1 Alexandra Road, Swansea SA1 5ED (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/090046 A2

(54) Title: INTRUSION DETECTION SYSTEM

(57) Abstract: An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorised party or entity to a computer system or network, the intrusion detection system comprising means for monitoring the activity relative to the computer system or network, means for receiving and storing one or more general rules, each of the general rules being representative of characteristics associated with a plurality of specific instances of intrusion or attempted intrusion, and matching means for receiving data relating to activity relative to said computer system or network from the monitoring means and for comparing, in a semantic manner, sets of actions forming the activity against the one or more general rules to identify an intrusion or attempted intrusion. Inductive logic techniques are proposed for suggesting new intrusion detection rules for inclusion into the system, based on examples of sinister traffic.